COMMVAULT

DATASHEET

Greater Data Protection: Immutable Backups to The Cloud With Commvault

Cyberthreats are rapidly increasing in sophistication and persistence. As threats increase, cyberattacks are expected to double by 2025.[1] What's more, if an organization is attacked, the average cost of downtime for large enterprises is more than $11,600 per minute.[2] Despite the increase in awareness and spending, it's estimated that every 11 seconds, an organization will be hit with a ransomware attack.[3] These statistics reinforce the importance of recovery readiness.

With cloud storage now a popular choice for offsite copies, data security becomes increasingly important, leading many data protection solutions to offer robust Write Once Read Many (WORM) and immutability options along with air gapping and isolation for stronger cloud protection and security.

Combining industry-leading security controls of Commvault Complete™ Backup & Recovery with cloud-based WORM and immutable storage integration can assure that your important data cannot be deleted, modified, or accessed by malicious cyber and internal threats while maintaining compliance with governing regulations.

AAA security framework controls

Commvault protects access, privacy, and control of backup data residing across copies, including those in the cloud. Commvault immutable backup data uses a rich feature set and incorporates AAA security framework principles:

AAA Security framework for controlling access

Authentication	Authorization	Accounting
Proving and granting access	Controlling authorized access levels	Tracking and auditing access and capabilities

Authentication controls provide and grant access to backup data. These gatekeeper features include certificate authentication, strong multi-factor authentication (MFA), and integration with multiple third-party identity providers using secure protocols such as LDAPS, SAML, and OpenID.

Authorization controls determine what level of access is allowed on the Commvault CommCell. Once authentication is granted, Commvault applies various controls such as role-based access controls (RBAC), multi-tenancy, data privacy locks, command authorization, and privileged access management platform integration. These features work in tandem to protect data from inappropriate access, retrieval, and deletion. Adding these gates create software isolation, where even administrators are blocked from deleting and accessing backup data as well as reversing security controls. Similarly, if a malicious actor steals access to the CommCell, backup data is secured from malicious activity within the Commvault platform.

1 Embroker: 2021 Must-Know Cyber Attack Statistics and Trends, December 2021
2 Web tribunal, Branko K., 15+ Scary Data Loss Statistics to Keep in Mind in 2022, March 2022
3 Cybercrime Magazine, Steve Morgan, Top 6 Cybersecurity Predictions and Statistics for 2021 To 2025, December 2021

Lastly, Commvault enforces accountability by auditing events and actions within the CommCell and providing a rich customizable interface and API with which to view this information. Hundreds of reports are readily available in the Commvault software store providing deep information on the operations, events, and actions of the CommCell. Report information and dashboards are only visible to authorized users, allowing owners to view the same audit reports and dashboards as administrators – without seeing resources they do not have permission to see. For continuous monitoring, Commvault leverages common protocols, platforms, and tools such as REST APIs, Syslog, Webhooks, SNMP, and SCOM – allowing support for any event monitoring system. Native plugins for Splunk and ServiceNow are also available for even more seamless integration. This further expands the accounting and audit capabilities within Commvault and provides flexibility to integrate with whatever systems are already in place within the organization.

Immutable cloud backups

Commvault Complete Backup & Recovery provides on-premises backup immutability by combining AAA framework security controls, hardening, data encryption, and native HyperScale™ X file system immutability. However, when designing a solution to protect against ransomware and cyberthreats, offsite copies of data are imperative.

When using cloud storage, such as Amazon Web Services (AWS) or Microsoft Azure, immutability options are enabled at the storage level with the cloud vendor. The cloud destination is configured as a library within Commvault for secondary and/or tertiary copies. When cloud immutability is enabled, all stored assets are locked, and the contents cannot be modified or deleted for the specified immutability time frame.

Using Commvault with immutable cloud storage has key advantages over other backup products:

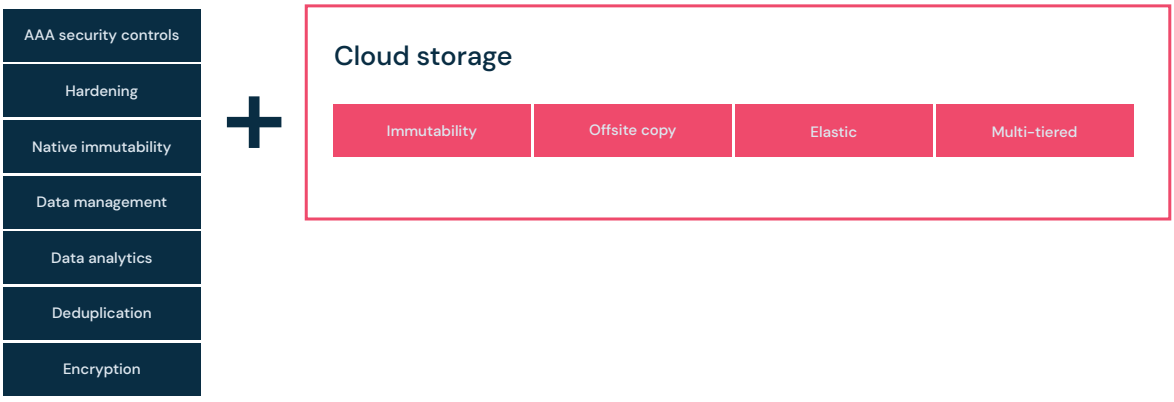
Commvault security controls and hardening

Commvault leverages the most secure Identity Access Management role-based authentication methods for cloud configurations. This eliminates any concerns over access keys getting lost or stolen, and prevents bad actors from gaining unauthorized access to cloud resources. From a backup management perspective, security controls applied as part of Commvault's AAA framework protect against accidents and malicious attempts to destroy protected data. Data that is immutable will stay immutable!

Deduplication

When faced with sending multi-petabytes of data to the cloud, cost and bandwidth dominate the conversation. Commvault software global deduplication begins where the source data resides. Only changed blocks are sent to the cloud, drastically reducing the bandwidth required for copy operations. This also allows more backup cycles (both full and incremental) to be protected in the cloud while reducing the storage footprint. Commvault's deduplication is applied globally across all servers and workloads within a policy, further optimizing the data footprint. Ultimately, Commvault deduplication allows backup copies to quickly get to the cloud, reducing recovery point objectives, increasing recovery readiness, and lowering storage footprint costs.

Commvault platform



Encryption and key management

Cloud storage encryption protects data at rest from being useful if stolen. However, this does not address source-side encryption needs. Commvault's FIPS 140-2 certified encryption module handles encryption at the source prior to sending data to the cloud. This ensures every block of data transmitted to the cloud is encrypted and secured. For more advanced security, encryption keys can be offloaded to external key management servers, including those from AWS, Azure, or any KMIP-compliant system.

Air gapping and isolation

Data isolation via air gapping is a great strategy for keeping data safe from laterally moving threats that may be active within your on-premises environment. Cloud storage is virtually air gapped by default since data is written and read to/from the cloud using authenticated API calls instead of using persistent network connections. Furthermore, with WORM/Object lock enabled on storage, data will remain unaffected from any changes in the event of compromised cloud management credentials.

Metallic® Recovery Reserve™

Metallic Recovery Reserve makes it easy to adopt secure and scalable cloud storage in just minutes, allowing you to meet the needs of your organization's hybrid cloud strategy without requiring additional cloud expertise within your organization. With Metallic Recovery Reserve, you can seamlessly adopt air-gapped cloud storage and gain predictable costs and reduced overhead. It can also be the foundation for improving your ransomware recovery strategy by leveraging a fully integrated, secondary cloud storage target for Commvault Backup & Recovery or Commvault HyperScale X.

Data management and analytics

Commvault manages retention and backup policies, while the cloud manages the immutable locks configured at the storage. Using a multi-tiered approach to storing data in the cloud, organizations can take advantage of cold storage options to save cost while having the index readily available on-premises or in warmer, more readily accessible cloud storage tiers for analytic purposes. Commvault allows cost-effective analysis of immutable cold storage backups, which can be leveraged for other business purposes. This capability and a consistent tiered approach can dramatically reduce cloud service providers' egress/access charges.

Regulatory compliance

Using cloud WORM and immutable storage options with Commvault helps organizations address SEC 17a-4(f), CFTC 1.31(d), FINRA, and other regulations related to the recording, storage, and retention requirements for electronic records. AWS[4] and Azure[5] are compliant storage options supported by Commvault, both designed to meet securities industry requirements for preserving records in a non-rewriteable and non-erasable format using their respective storage-locking technologies.

Conclusion

Keep pace and mitigate risk – even while cyberthreats are increasing. With highly available cloud storage and greater security protection, it's simple to start creating secondary and tertiary data copies. Without any extra costs, Commvault Complete Backup & Recovery will manage, analyze, and secure your backup data efficiently, while cloud immutability further locks data from cyberthreats – today and in the future. With Commvault, you have the security and protection to store and manage your data on premises and in the cloud. Are you recovery ready?

4 Amazon Glacier with Vault Lock: SEC 17a-4(f) and CFTC 1.31(b)-(c) Compliance Assessment
5 Microsoft Azure Storage: SEC 17a-4(f) and CFTC 1.31(c)-(d) Compliance Assessment